(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 March 2004 (25.03.2004)

PCT

(10) International Publication Number
WO 2004/025895 A1

(51) International Patent Classification[7]: H04L 9/32, 29/06, 9/00

(21) International Application Number: PCT/EP2002/010400

(22) International Filing Date: 13 September 2002 (13.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S.12625 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AHONEN, Pasi** [FI/FI]; Salotie 5, FIN-90630 Oulu (FI). **UUSITALO, Ilkka** [FI/FI]; Palosuontie 6 b 6, FIN-90800 Oulu (FI). **MÄNTYLÄ, Vesa-Matti** [FI/FI]; Koskitie 26 A 8, FIN-90500 Oulu (FI).

(74) Agents: **LIND, Robert** et al.; Marks & Clerk, 4220 Nash Court, Oxford Business Park South, Oxford, Oxfordshire OX4 2RU (GB).

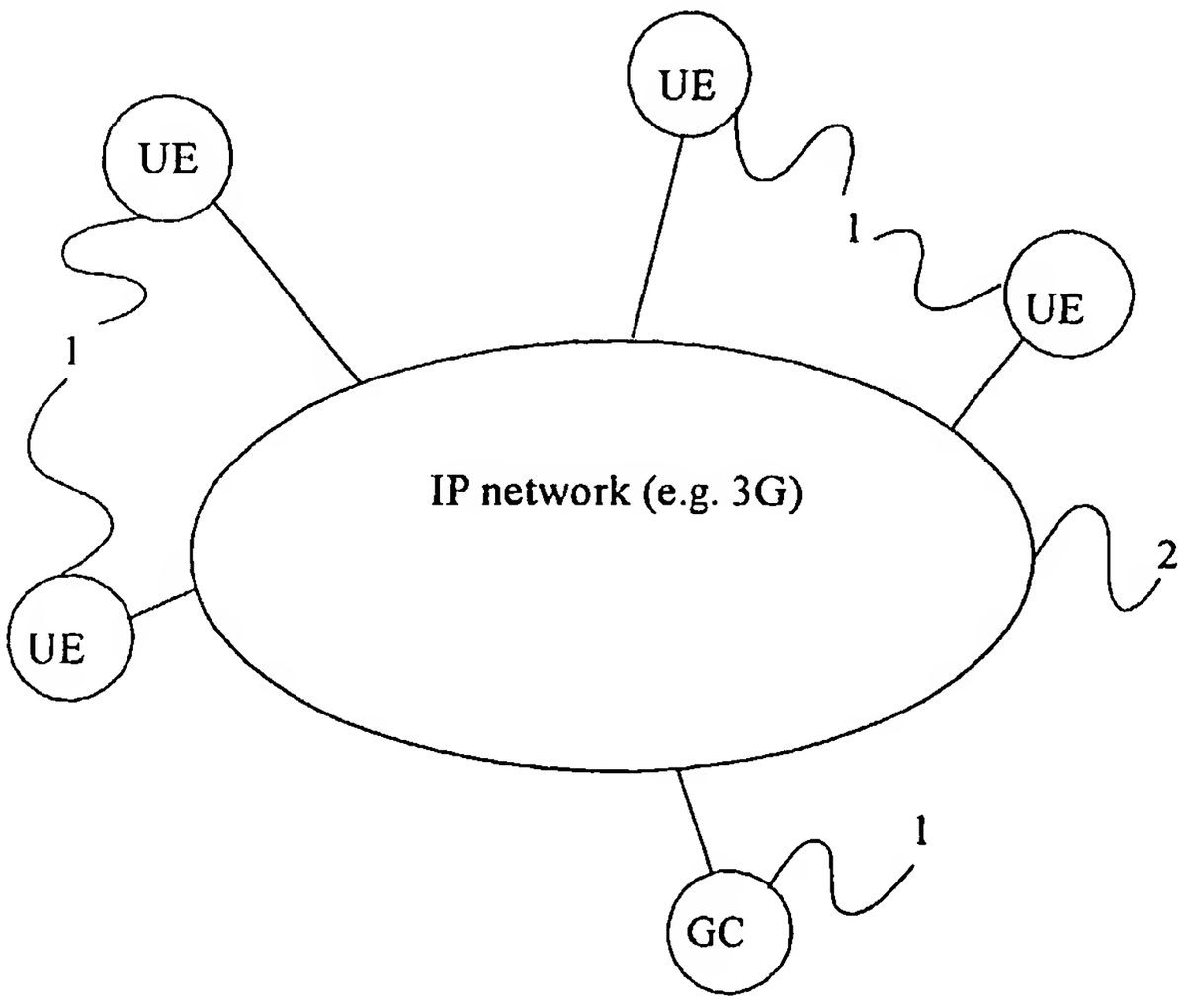
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SECURE BROADCAST/MULTICAST SERVICE



(57) Abstract: A method of authenticating candidate members 1 wishing to participate in an IP multicast via a communication network, where data sent as part of the multicast is to be encrypted using a Logical Key Hierarchy based scheme requiring that each candidate member submit a public key to a group controller. The method comprises, at the group controller 1, verifying that the public key received from each candidate member 1 is owned by that member and that it is associated with the IP address of that candidate member 1 by inspecting an interfaceID part of the IP address.

WO 2004/025895 A1